

REMARKS

The application has been amended and is believed to be in condition for allowance.

Claims 17-21 are new.

The independent claims have been amended to address the Section 112, 2nd paragraph, rejection. Withdrawal of this rejection is therefore solicited.

There are no other formal matters outstanding.

Claims 9-16 were rejected as obvious over FRANCISCO et al. 5,263,147 in further view of CLIFTON 5,469,556.

As to the independent claims, e.g., claim 9, the Official Action indicates that FRANCISCO is failing only to disclose "that the security device processor had access to the resources or the security device processor executed the security critical activity".

Claim 9 is reproduced below with annotations indicating how the claim is being read onto FRANCISCO, with reference to Figure 1. System [comprising] a processor (cpu 1 of base cpu card), handling devices (keyboard 25, memory storage means (memory 30), hereafter named resources.

FRANCISCO is also offered as disclosing a security device (security computer 31 and access monitoring unit 100) comprising a processor (cpu 7 of security cpu card 28) and signal generators (amu hardware control 321 of Figure 3), a number of control means, hereafter named switches (amu hardware 325), with

signal receivers (column 5, paragraph 6, asserted to be inherently disclosed therein). Figure 3 shows a block diagram of the software components of the FRANCISCO system.

Claim 9 recites that the signal receivers are arranged respectively between the security device and pre-selected resources (31, 100, and 30), that the switches contain information regarding accessibility to and from the resources, or parts of the resources, hereafter named resource ranges (amu memory 102 of base cpu card 27).

Claim 9 continues by reciting in that the security processor is arranged to execute the security critical activity, that the switch controls requests from a processor of the computer to the resources or resource ranges depending on the information contained in the switch amu memory 102, column 2, paragraphs 2-3), and that in response to a call from the computer processor or the handling devices, the switches are activated by receiving a signal (??) from the security device, enabling the security device and its processor access to and from the resources or resource ranges selected by the security device and **denying the computer processor access to and from the resources or resource ranges selected by the security device** (column 4, paragraph 3, claim 1), in that the signal (SG_{PM}) can be generated only by the security device (column 5, paragraph 6, lines 1-4) and in that the security device comprises a signal generator

(??). Applicant does not see that the "denying" recitation is satisfied by FRANCISCO.

The wherein clause recited, wherein, when a switch receives a signal (SG_A), together with new information (addresses, operation, data), the security device is able of altering a content of the information of that switch (column 5, lines 39-50).

The Official Action thus acknowledges that FRANCISCO fails to disclose "that the security device processor had access to the resources or the security device processor executed the security critical activity".

CLIFTON is offered as teaching "that in a computing system it is desirable to have classify certain instructions as secure and others as unsecure and to have a normal processor execute the unsecure instructions and a secure processor to processor to execute the secure instructions" (OA page 5, top paragraph).

Applying the teachings of CLIFTON to FRANCISCO, would result in assigning the processor 1 of the base cpu card 27 with the unsecure instructions/tasks and assigning the processor 7 of the security cpu card with the secure instructions/tasks.

However, this modification still falls short of having FRANCISCO teach each feature of the invention as claimed.

From claim 9 again see the recitation "in that in response to a call from the computer processor or the handling

devices, **the switches are activated by receiving a signal (SG_{PM}) from the security device**, enabling the security device and its processor access to and from the resources or resource ranges selected by the security device and denying the computer processor access to and from the resources or resource ranges selected by the security device, in that the signal (SG_{PM}) can be generated only by the security device and in that the security device comprises a signal generator (SG_A),".

Page 4 of the Official Action, lines 9-16 are relevant. For the language "in response to a call from the computer processor or the handling devices, **the switches are activated by receiving a signal from the security device**, enabling the security device and its processor access to and from the resources or resource ranges selected by the security device and **denying the computer processor access to and from the resources or resource ranges selected by the security device**" the Official Action offers FRANCISCO column 4, paragraph 3, and claim 1.

Column 4, paragraph 3 discloses that "The base computer system can, in preferred embodiments, use MS-DOS, O/S 2 or UNIX operating systems. Conventional operating system functions are presented with a security system-emulated operating system compatible file system. In preferred embodiments, other utility programs are provided for managing and displaying the security system's object attributes maintained by the security system."

This passage discloses utility programs managing the security system functions, but does not disclose any "denying" action *as a result of the switches receiving a signal from the security device.*

FRANCISCO Claim 1, reads (emphasis added): "1. A security system for use with a computer system having a processing unit and memory comprising: an access monitor unit connected between the processing unit and the memory of said computer system for continuously monitoring all operations between the memory and the processing unit of the computer system; security means for controlling the operation of said access monitoring unit **to allow or deny access to the memory by the processing unit based on predefined security conditions;** and security computer means communicating with said access monitoring unit for implementing said security means and controlling said access monitoring unit."

Thus, there is disclosed denying access to the memory, but this functionality is based on predefined security conditions and not any dynamic restriction set by the security processor. The predefined security conditions, as offered by Official Action page 4, lines 14-15, is that the subject is denied access when they are requesting an access outside the subject's access rights. But there is no disclosure of restricting access to the normal processor in response to switches receiving a signal from the security processor.

Further, CLIFTON does not teach this missing feature. CLIFTON does not make any teaching as to a security device that sends signals to a switch so as to restrict access to the switch to the security processor (denying access to the normal processor).

The independent claims have been amended to make more clear that it is the signal (SG_{PM}) from the security device that activates the switches to be in a condition:

i) enabling the security device and its processor access to and from the resources or resource ranges selected by the security device and

ii) denying the computer processor access to and from the resources or resource ranges selected by the security device.

There is no such teaching in the applied references.

Accordingly, the independent claims are believed patentable over the prior art.

Reference is made to Figure 2 and specification page 8.

Claim 14 has been amended to recite that the switches are configured for i) a first normal mode wherein the processor has access to the resources, and ii) a second protected mode wherein the processor is denied access to the resources but the security processor is allowed access, and that said signal from the security device (that enables the security device and its process access to the resources and denies the computer processor access to the resources), changes the switches from the first

normal mode into the second protected mode. See similar claims 17-18.

This feature of the invention is also both novel and non-obvious over the prior art.

New claims 19-21 recite that the switches each comprise a protection mode signal receiver (SR) configured to receive said signal from the security device activating the switches to be in the condition enabling the security device and the security processor access to the resources and denying the computer processor access to the resources. These claims further recite that upon reception of said signal from the security device by the protection mode signal receiver, the protection mode signal receiver reconfigures the switches into a protection mode configuration allocating specific resources needed for executing the security critical activity to the security processor and denying the computer processor access to the specific resource. Lastly, these claims recite that upon the switches being placed in the protection mode configuration, the security processor executes the security critical activity.

The prior art also does not teach these features of the invention.

Summary

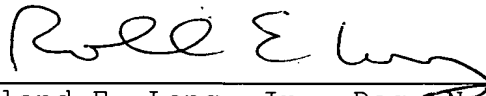
Thus, unlike FRANCISCO or CLIFTON (individually or in combination), according to the present invention, switches are placed in a condition such that a security critical activity is executed by the processor of the security device, while the processor of the computer is denied access to the resources used by the security device for executing the security critical activity.

For the reasons outlined above, the applied reference is not believed to be anticipatory and the claims are believed allowable. Accordingly, reconsideration and allowance of all the pending claims are respectfully requested.

The Commissioner is hereby authorized in this, concurrent, and future replies, to charge payment or credit any overpayment to Deposit Account No. 25-0120 for any additional fees required under 37 C.F.R. § 1.16 or under 37 C.F.R. § 1.17.

Respectfully submitted,

YOUNG & THOMPSON



Roland E. Long, Jr., Reg. No. 41,949
745 South 23rd Street
Arlington, VA 22202
Telephone (703) 521-2297
Telefax (703) 685-0573
(703) 979-4709

REL/lk